

Title (en)
METHOD, APPARATUS AND ARTICLE FOR IDENTIFICATION AND SIGNATURE

Publication
EP 0252499 B1 19921007 (EN)

Application
EP 87109861 A 19870708

Priority
US 88324786 A 19860709

Abstract (en)
[origin: EP0252499A2] A method and apparatus for simple identification and signature which enable any user to prove his identity and the authenticity of his messages to any other user. The method and apparatus are provably secure against any known or chosen message attack if factoring is difficult, and require only 1% to 4% of the number of modular multiplications previously required. The simplicity, security and speed of the method and apparatus derive from microprocessor-based devices which may be incorporated into smart cards, personal computers, passports, and remote control systems.

IPC 1-7
G07F 7/10; H04L 9/00

IPC 8 full level
G06K 17/00 (2006.01); **G06Q 20/34** (2012.01); **G06Q 20/40** (2012.01); **G06Q 40/00** (2006.01); **G07F 7/10** (2006.01); **G09C 1/00** (2006.01); **H04L 9/00** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)
G06Q 20/341 (2013.01 - EP US); **G06Q 20/40975** (2013.01 - EP US); **G07F 7/1008** (2013.01 - EP US); **G07F 7/1016** (2013.01 - EP US); **H04L 9/3073** (2013.01 - EP US); **H04L 9/3221** (2013.01 - EP US); **H04L 2209/56** (2013.01 - EP US)

Citation (examination)
GOLDWASSER, MICALI, RACKHOFF " The knowledge Complexity of Inter active Proof-Systems", ACM 0-89791-Pages291-304

Cited by
AU712668B2; US5434917A; EP0311470A1; EP0505302A1; US5867577A; US5452357A; EP0325238A3; US4944007A; AU622915B2; FR2728981A1; EP0583709A1; FR2773406A1; EP0661846A1; FR2714780A1; US5581615A; EP1056241A3; WO2012150396A2; US6226382B1; WO9620461A1; EP1573957A1

Designated contracting state (EPC)
AT BE CH DE FR GB IT LI NL SE

DOCDB simple family (publication)
EP 0252499 A2 19880113; EP 0252499 A3 19890712; EP 0252499 B1 19921007; AT E81414 T1 19921015; AU 592207 B2 19900104; AU 7526687 A 19880114; DE 3782099 D1 19921112; DE 3782099 T2 19930211; IL 83095 A 19910415; JP 2511464 B2 19960626; JP S63101987 A 19880506; US 4748668 A 19880531

DOCDB simple family (application)
EP 87109861 A 19870708; AT 87109861 T 19870708; AU 7526687 A 19870706; DE 3782099 T 19870708; IL 8309587 A 19870706; JP 17202587 A 19870709; US 88324786 A 19860709